MAT-8749US PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Hidekazu SUZUKI : Art Unit:
Serial No.: 10/549,423 : Examiner:
Filed: September 15, 2005
FOR: REVOCATION INFORMATION TRANSMISSION METHOD, RECEPTION METHOD, AND DEVICE THEREOF

VERIFICATION OF A TRANSLATION

Assistant Commissioner for Patents
Washington, D.C. 20231
SIR :

I, the below named translator, hereby declare that:

1. My name and post office address are as stated below.

2. That I am knowledgeable in the English language and in the language of JP2003-085043, and I believe the attached English translation to be a true and complete translation of JP2003-085043.

3. The document for which the attached English translation is being submitted is a patent application on an invention entitled REVOCATION INFORMATION TRANSMISSION METHOD, RECEPTION METHOD, AND DEVICE THEREOF.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Date: May 19, 2011

Katsuyuki Hirano

Full name of the Translator

K. Hirano

Signature of the Translator

6-5-24, Danjo-cho, Nishinomiya-shi, Hyogo 663-8006 Japan

Post Office Address

[NAME OF THE DOCUMENT] Patent Application
[ARRANGEMENT NUMBER] 2113140223
[DATE OF FILING] March 26, 2003
[ADDRESS] Director-General of the Patent Office
[INTERNATIONAL PATENT CLASSIFICATION] H04N 7/167
H04K 1/00
G06F 12/14 320

[INVENTORS]
[ADDRESS] c/o Matsushita Electric Industrial Co., Ltd.
1006, Oaza-Kadoma, Kadoma-shi, Osaka
[NAME] Hidekazu SUZUKI
[APPLICANT]
[IDENTIFICATION NUMBER] 000005821
[NAME] Matsushita Electric Industrial Co., Ltd.
[AGENT]
[IDENTIFICATION NUMBER] 100097445
[NAME] Fumio IWAHASHI, Patent Attorney
[SELECTED AGENT]
[IDENTIFICATION NUMBER] 100103355
[NAME] Tomoyasu SAKAGUCHI, Patent Attorney
[SELECTED AGENT]
[IDENTIFICATION NUMBER] 100109667
[NAME] Hiroki NAITO, Patent Attorney

[REPRESENTATION OF FEE]
[NUMBER IN LEDGER OF IN-ADVANCE PAYMENT] 011305
[AMOUNT] 21,000 yen
[LIST OF ARTICLES FILED]
[NAME OF ARTICLE] Specification 1
[NAME OF ARTICLE] Drawing 1
[NAME OF ARTICLE] Abstract 1
[NUMBER OF GENERAL POWER OF ATTORNEY] 9809938

[Name of the Document] Specification

[Title of the Invention] Revocation information transmission method, reception method, and device thereof.

[Claims]

[Claim 1] A revocation information transmission method to be used in a system comprising a contents transmitting device for sending out contents, a contents receiving device for receiving contents, and connecting means for connecting between the contents transmitting device and the contents receiving device, comprising a step of executing mutual authentication between the contents transmitting device and the contents receiving device, a step of uploading, in case of failure of mutual authentication, revocation information including key information failing in mutual authentication, from the contents transmitting device or the contents receiving device, a step of preparing integrated revocation information by integrating individual revocation information uploaded from a plurality of contents transmitting devices or contents receiving devices, a step of packetizing the integrated revocation information and multiplexing it into a stream, and a step of transmitting the multiplexed stream of integrated revocation information.

[Claim 2] A revocation information transmission method comprising a step of preparing integrated revocation information by integrating individual revocation information from a single or a plurality of contents transmitting devices or contents receiving devices, a step of

packetizing the integrated revocation information and multiplexing it into a stream, and a step of transmitting the multiplexed stream of integrated revocation information.

[Claim 3] The revocation information transmission method of claim 1 or 2, wherein the integrated revocation information is transmitted by using a data structure of section of MPEG transport stream.

[Claim 4] The revocation information transmission method of claim 1 or 2, wherein the integrated revocation information is transmitted by using a data structure of PES packet of MPEG transport stream.

[Claim 5] The revocation information transmission method of claim 1 or 2, wherein the integrated revocation information is transmitted by using a payload of transport packet of MPEG transport stream.

[Claim 6] The revocation information transmission method of claim 1 or 2, wherein the integrated revocation information is transmitted by using an IP packet.

[Claim 7] A revocation information reception method comprising the steps of receiving an integrated revocation list by a contents transmitting device or a contents receiving device, and storing the integrated revocation list by the contents transmitting device or the contents receiving device.

[Claim 8] A revocation information transmitting apparatus comprising a plurality of contents transmitting devices for sending out contents, a plurality of contents receiving devices individually connected to the plurality of contents transmitting devices for receiving the contents, connecting means for connecting between the contents transmitting devices and the contents receiving devices, a network for sucking up revocation

information from the plurality of contents transmitting devices or the plurality of contents receiving devices, integrating means connected to the network for integrating the revocation information, multiplexing means for packetizing the integrated revocation information integrated in the integrating means and multiplexing it into a stream, and transmitting means for transmitting the stream multiplexed in the multiplexing means.

[Claim 9] A revocation information transmitting apparatus comprising integrating means for integrating individual revocation information from a single or a plurality of contents transmitting devices or contents receiving devices, multiplexing means for packetizing the integrated revocation information integrated in the integrating means and multiplexing it into a stream, and transmitting means for transmitting the stream multiplexed in the multiplexing means.

[Claim 10] The revocation information transmitting apparatus of claim 8 or 9, wherein the integrated revocation information is transmitted by using a data structure of section of MPEG transport stream.

[Claim 11] The revocation information transmitting apparatus of claim 8 or 9, wherein the integrated revocation information is transmitted by using a data structure of PES packet of MPEG transport stream.

[Claim 12] The revocation information transmitting apparatus of claim 8 or 9, wherein the integrated revocation information is transmitted by using a payload of transport packet of MPEG transport stream.

[Claim13] The revocation information transmitting apparatus of claim 8 or 9, wherein the integrated revocation information is transmitted by using an IP packet.

[Claim 14] A revocation information receiving apparatus comprising the steps of receiving an integrated revocation list by a contents transmitting device or a contents receiving device, and storing the integrated revocation list by the contents transmitting device or the contents receiving device.

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

The present invention relates to a revocation information transmission method and apparatus thereof for preventing digital pictures or digital voices from being displayed or reproduced by unjust electronic apparatuses.

[0002]

[Background Art]

In recent years, along with development in digital technology, popularity is increasing about digital broadcast, digital contents distribution by the Internet, and digital contents distribution and accumulation by DVD, hard disk or card memory. Since digital data are used in these media, it is possible to copy the data without deterioration in quality, but from the viewpoint of protection of copyright, it is important to realize security for preventing such illegal copying. For realizing the security, it is necessary to issue revocation information, that is a so-called black list of unjust apparatuses, when an apparatus is found to be unjust from the viewpoint of protection of copyright, so the apparatus that can be connected to an unjust apparatus may have the revocation information, thereby preventing unfair

access to digital contents.

[0003]

Fig. 25 shows an example of configuration of a conventional system for renewing of revocation information (see, for example, patent document 1).

[0004]

Reference numeral 1 is a contents sales system, which is an automatic vending machine for electronically distributing music contents via a communication network such as broadcast or the Internet. Reference numeral 2 is an electric music distributor (EMD), which is actually a music server or a music broadcasting station. Reference numeral 3 is a revocation information issuing authority. Reference numeral 4 is a secure contents server. Reference numeral 5 is a revocation information storage section, which receives the revocation information issued by the revocation information issuing authority. Reference numeral 6 is a music data storage section, which stores music data. Reference numeral 7 is a license storage section, which stores a key for decoding coded contents. Reference numeral 8 is an EMD I/F, which is an interface for receiving coded contents. Reference numeral 9 is a PF I/F, which is an interface for connecting with PD 12. Reference numeral 10 is media I/F, which is a card slot of PCMCIA for mounting PM 13. Reference numeral 11 is storage media or portable media (PM). Reference numeral 12 is a playback device (PD). Reference numeral 13 is a user I/F, which is an interface to be operated by the user.

[0005]

Patent document 1

Japanese Patent Unexamined Publication No. 2001-166996

[0006]

[Problems to be Solved by the Invention]

In this background art, however, nothing specific is mentioned about method distribution of revocation information although the renewing method of revocation information is described, and it is required to distribute revocation information in the recent background of heightening of contents distribution by digital broadcast or the Internet.

[0007]

[Means to Solve the Problems]

The present invention is hence devised in order to solve these conventional problems, and it is hence a primary object of the present invention (as set forth in claim 1) is to provide a revocation information transmission method which is used in a system including a contents transmitting device for sending out contents, a contents receiving device for receiving contents, and connecting means for connecting between the contents transmitting device and the contents receiving device, which includes a step of executing mutual authentication between the contents transmitting device and the contents receiving device, a step of uploading, in case of failure of mutual authentication, revocation information including key information failing in mutual authentication, from the contents transmitting device or the contents receiving device, a step of preparing integrated revocation information by integrating individual revocation information uploaded from a plurality of contents transmitting devices or contents receiving devices, a step of packetizing the integrated revocation information and multiplexing it into a stream, and a step of transmitting the

multiplexed stream of integrated revocation information.

[0008]

The present invention (as set forth in claim 7) is to provide a revocation information reception method including the steps of receiving an integrated revocation list by a contents transmitting device or a contents receiving device, and storing the integrated revocation list by the contents transmitting device or the contents receiving device.

[0009]

The present invention (as set forth in claim 8) is to provide a revocation information transmitting apparatus including a plurality of contents transmitting devices for sending out contents, a plurality of contents receiving devices individually connected to the plurality of contents transmitting devices for receiving the contents, connecting means for connecting between the contents transmitting devices and the contents receiving devices, a network for sucking up revocation information from the plurality of contents transmitting devices or the plurality of contents receiving devices, integrating means connected to the network for integrating the revocation information, multiplexing means for packetizing the integrated revocation information integrated in the integrating means and multiplexing it into a stream, and transmitting means for transmitting the stream multiplexed in the multiplexing means.

[0010]

The present invention (as set forth in claim 14) is to provide a revocation information receiving apparatus including the steps of receiving an integrated revocation list by a contents transmitting device or a contents

receiving device, and storing the integrated revocation list by the contents transmitting device or the contents receiving device.

[0011]

[Description of the Preferred Embodiments]

(Preferred embodiment 1)

Referring now to the accompanying drawings, preferred embodiment 1 of transmission method and reception method of revocation information of the present invention is described specifically below. Fig. 1 shows a system configuration for realizing the transmission and reception methods of revocation information in preferred embodiment 1 of the present invention. Reference numerals 101 to 109 represent general electric household appliances. Reference numeral 101 is a first display, such as CRT, liquid crystal display or plasma display, which displays pictures, and is sometimes provided with a speaker for delivering voice signals.

[0012]

Fig. 2 shows an internal configuration of first display 101. Reference numeral 1001 is a display unit for displaying pictures. Reference numeral 1002 is an apparatus interface for connecting with an STB described later. Reference numeral 1003 is a control unit of the display, which controls the entire display. Reference numeral 1004 is a memory unit, which stores maker ID, apparatus ID and key information of the display described later.

[0013]

Reference numeral 102 is a first set-top box (STB), which receives, decodes, and reproduces distributed or broadcast digital pictures, voices, and

other data. Herein, the STB is supposed to receive digital broadcast.

[0014]

Fig. 3 shows an internal configuration of the STB. Reference numeral 1101 is an antenna, which receives digital broadcasting waves. Reference numeral 1102 is a tuner unit, which demodulates broadcasting waves. Reference numeral 1103 is a front end unit, which corrects errors with respect to the demodulated signals, and reproduces a transport stream (TS). Reference numeral 1104 is a TS decoder unit, which extracts user-selected program packets (picture, voice, data, etc.) from TS multiplexed with a plurality of programs. Reference numeral 1105 is an AV decoder unit, which elongates the picture packet and voice packet extracted by TS decoder unit 1104, and sends out the digital picture signal and voice signal. Reference numeral 1106 is a control unit, which controls the entire STB. Reference numeral 1107 is a memory unit, which stores revocation list and STB key information described later. Reference numeral 1108 is a display interface, which sends out pictures and voices to the display, or exchanges key information. Reference numeral 1109 is a modem unit, which communicates with network 113 described later.

[0015]

Reference numeral 103 is a digital interface, which connects between the first display and the first STB. This is an example of HDMI (high-definition multimedia interface). Reference numeral 104 is a second display, which is similar to first display 101. Reference numeral 105 is a second STB, which is similar to first STB 102. Reference numeral 106 is a second digital interface for connecting between the second display and the

second STB, which is similar to first digital interface 103.

[0016]

Reference numeral 107 is an N-th display (N being a natural number), which is similar to first display 101. Reference numeral 108 is an N-th STB, which is similar to first STB 102. Reference numeral 109 is an N-th digital interface, which is similar to first digital interface 103.

[0017]

Reference numeral 110 is a first up-line for connecting between first STB 102 and a network described later, which is a medium for transmitting the revocation list accumulated in the STB to the network. The revocation list is specifically described later. The up-line is a copper wire, optical cable or the like.

[0018]

Reference numeral 111 is a second up-line, which is similar to first up-line 110. Reference numeral 112 is an N-th up-line, which is similar to first up-line 110. Reference numerals 101 to 112 are available at each home or individually put into available form at each home, and the N-th value is not limited.

[0019]

Reference numeral 113 is a network, which is a medium, such as a telephone network or the Internet, for sucking up the revocation list from the STB at each home into a revocation list integrator. Reference numeral 114 is a revocation list integrator, which integrates the revocation list sucked up from each STB in order to prepare and control the integrated revocation list that is a table of revocation lists. Reference numeral 115 is a transmitting

center, which packetizes the integrated revocation list and multiplies it into a transport stream for broadcast. Reference numeral 116 is a transmitter unit, which is, for example, a transmitting antenna for transmitting to each STB.

[0020]

In preferred embodiment 1 having such configuration, the operation is specifically described below. The HMDI operates on an encoding system known as HDCP (high-bandwidth digital content protection). The HDCP prescribes the encoding method for digital contents which flow between a transmitting apparatus such as an STB, DVD or the like for transmitting pictures and voices, and a receiving apparatus such as a display unit for displaying pictures. The detail is mentioned in the standard book of HDCP, High-Bandwidth Digital Content Protection System, and the detail is omitted herein.

[0021]

The first to N-th displays have maker ID, apparatus ID, and a matrix of device keys for display of 56 bits x 40 lines in each memory unit 1104. It is shown in Fig. 4. Corresponding to the matrix of device keys, a key selection vector (KSV) is assigned for specifying the line of each device key, and is stored in memory unit 1107. Hereinafter, a KSV for display is referred to as Bksv.

[0022]

The first to N-th STBs also have device keys and KSV for STB in each memory unit 1104. Hereinafter, a KSV for STB is referred to as Aksv.

[0023]

The device key and key selection vector are controlled by LLC, which is a control organization of HDCP, and are given to apparatuses such as each display, STB and DVD.

[0024]

A method of preparing a revocation list at each STB is described below. As an example, first STB 102 and first display 101 are explained. Fig. 5 shows a process for initial authentication of STB and display. The detail of this process is described in the above-mentioned book, High-Bandwidth Digital Content Protection System, and the detail is omitted herein. Fig. 6 shows an example of revocation list of memory unit 1107 of the first STB. This list stores maker ID, apparatus ID, and Bksv of the display to be excluded as an unjust apparatus from the viewpoint of protection of copyright. In the example in Fig. 6, two displays are registered as apparatuses to be excluded. The maker ID is an identification of a manufacturer. The apparatus ID is an identification of an apparatus, which is, for example, a serial number of the apparatus.

[0025]

Initial authentication is described below. Firstly, first STB 102 and first display 101 are connected to each other by first digital interface 103, or first STB 102 and first display 101 are supplied with power.

[0026]

Next, first STB 102 reads out the maker ID, apparatus ID, and Bksv out of first display 101 via first digital interface 103. At this time, it is preferable to use an I2C line, which is a control line of the first digital interface.

[0027]

In this case, if the maker ID, apparatus ID, and Bksv being read out herein are same as those of the revocation list of the first STB, it is a failure of initial authentication, and this display cannot be used thereafter.

[0028]

Then, random number An of 64 bits, and Aksv are written into first display 101 from first STB 102 via first digital interface 103.

[0029]

Herein, it is also preferable to use the I2C line.

[0030]

Next, first STB 102 reads out Bksv out of first display 101, and executes the following calculation (formula 1) at the first STB.

[0031]

(formula 1)

$Km = \Sigma Akeys \text{ over } Bksv$

[0032]

The calculation (formula 1) is explained. Akeys is a matrix of STB's device keys of 56 bits x 40 lines, which is stored in memory unit 1107 of STB. For example, supposing Bksv to be 0 x 2B8 in a hexadecimal expression, starting from zero, only bit positions 3, 4, 5, 7, and 9 are "1", and others are "0".

[0033]

In the above formula, bit positions 3, 4, 5, 7,and 9 where "1" of Bksv exists are the indexes of lines, and five 56-bit keys are added.

[0034]

In first display 101, similarly, the calculation (formula 2) is executed.

[0035]

(formula 2)

Km' = ΣBkeys over Aksv

[0036]

Bkeys is a matrix of display's device keys of 56 bits x 40 lines, which is stored in memory unit 104 of the display.

[0037]

On the basis of Km, the STB executes the calculation (formula 3), and obtains Ks, M0, and R0.

[0038]

(formula 3)

(Ks, M0, R0) = hdcpBlkCipher (Km, REPEATER | | An)

[0039]

In formula 3, REPEATER is "1" when the relevant apparatus performs the repeat function, that is, re-transmission function, and it is "0" otherwise. Here, it is supposed that the display has no repeat function, and it is "0". In formula 3, "| |" shows a bit linkage. The operator called "hdcpBlkCipher" used in formula 3 is descried in detail in Chapter 4.5 of the document High-Bandwidth Digital Content Protection System, and the detail is omitted herein.

[0040]

On the other hand, the calculation (formula 4) is similarly executed in the display.

[0041]

(formula 4)

(Ks', M0', R0') = hdcpBlkCipher (Km', REPEATER | | An)

[0042]

The next process is to determine the initial authentication, and it is shown in Fig. 7. Specifically, the STB reads R0' out of the display, and determines whether R0 = R0' or not. In case R0 is coincident with R0', the initial authentication is successful. On the other hand, in case R0 is not coincident with R0', it is regarded as a failure of initial authentication, and the STB regards the display's Bksv to be unjust and registers it in the revocation list of memory unit 1107. At this time, the maker ID and the apparatus ID are stored at the same time. Fig. 8 shows the detail of memory unit 1107 at this time. In Fig. 8, maker_3, kiki_3, and Bksv_3 are newly registered as unjust apparatuses.

[0043]

The detail of the initial authentication process is described in the document High-Bandwidth Digital Content Protection System, and the detailed description is omitted herein. The second to N-th STBs, and the second to N-th displays also execute similar initial authentication processing same as the first STB and the first display, and if any Bksv is found to be unjust, it is registered in the revocation list of the memory unit of the STB connected thereto.

[0044]

A method of integrating the revocation list registered in each STB, and transmitting it to each STB is described below. Fig. 9 shows a flow ranging from uploading to transmitting of the revocation list.

[0045]

In step 101,

control unit 1106 of the STB reads maker ID, apparatus ID, and Bksv out of the revocation list stored in memory unit 1107, and transfers them to modem unit 1109.

[0046]

In step 102,

Bksv is uploaded from modem unit 1109 of the STB to revocation list integrator 114 via up-line 110 and network 113.

[0047]

In step 103,

a list of Bksv uploaded from each STB during a predetermined period is prepared at revocation list integrator 114, which is obtained as an integrated revocation list.

[0048]

In step 104,

the integrated revocation list is transmitted from revocation list integrator 114 to transmitting center 115.

[0049]

In step 105,

transmitting center 115 packetizes the integrated revocation list and multiplexes it into a transport stream.

[0050]

In step 106,

Transmitter 116 transmits the transport stream multiplexed with

the integrated revocation list to each STB.

[0051]

The following is a detailed description of packetizing and multiplexing of revocation list in step 105. Fig. 10 schematically shows a transport packet, and Fig. 11 shows a data structure of the transport packet. The data structure of transport packet is described in the MPEG system standard, ISO/IEC13818-1, and the description is omitted.

[0052]

The integrated revocation list is stored in the payload portion of the transport packet, that is, in the data_byte portion in Fig. 10, in which a certain PID is assigned. The PID is, for example, Revocation_pid. In preferred embodiment 1, the integrated revocation list is stored in a section structure conforming to MPEG system standard. Fig. 12 shows an example of data structure when the integrated revocation list is stored in a section structure. The table of integrated revocation list is called, for example, Revocation_list_table, but the name may be arbitrary. In this data structure, maker_id (16 bits), kiki_id (32 bits), and device_KSV (40 bits) are the maker ID, apparatus ID, and each unjust Bksv sucked up from the STB. However, the maker ID and the apparatus ID are not particularly limited in the number of bits.

[0053]

A method of receiving an integrated revocation list at each STB is described below. Fig. 13 shows a flow of receiving an integrated revocation list at the STB.

[0054]

In step 201,

STB receives TS (transport stream) including Revocation_list_table.

[0055]

In step 202,

control unit 1106 sets the Revocation_pid to a PID filter of TS decoder 1104 so as to extract a packet including Revocation_list_table from the TS at TS decoder 1104 of STB. The PID filter is for extracting a packet having a specified PID, and it is an essential function for the TS decoder.

[0056]

In step 203,

TS decoder unit extracts a packet including Revocation_list_table, and control unit 1106 obtains an integrated revocation list.

[0057]

In step 204,

control unit 1106 stores the obtained integrated revocation list in memory unit 1107.

[0058]

Fig. 14 shows the integrated revocation list stored in memory unit 1107. In this way, it becomes possible for all STBs to have an integrated revocation list in common.

[0059]

When a new display is connected to an STB, the operation is as follows: if the maker ID, apparatus ID, and Bksv being read out from the display coincide with those in the revocation list stored in the memory unit of the STB, the initial authentication is a failure, and the display is not usable

thereafter.

[0060]

According to preferred embodiment 1, as described herein, the apparatus is judged to be unjust if failing in the initial authentication process of the STB and the display, and the maker ID, apparatus ID, and KSV of the unjust apparatus are stored in the memory unit of the STB, and a revocation list is prepared, and from each STB, a revocation list is uploaded to the revocation list integrator via the network, and the revocation lists uploaded from the individual STBs are integrated in the revocation list integrator, and are packetized into a section, and it is multiplexed into a TS, and the multiplexed TS is sent out from the transmitter, and the TS transmitted from the transmitter is received in the STB, and thereby an integrated revocation list is obtained, so that the revocation lists individually owned in each STB can be commonly possessed in all STBs, and unjust displays from the viewpoint of protection of copyright can be excluded, and the security can be enhanced.

[0061]

(Preferred embodiment 2)

Next, preferred embodiment 2 of transmission method and reception method of revocation information of the present invention is described specifically below. What differs from preferred embodiment 1 lies in the method of packetizing the integrated revocation list. Fig. 15 shows a data structure of a packet including an integrated revocation list in preferred embodiment 2. In preferred embodiment 2, as shown in Fig. 14, an integrated revocation list is stored in a PES packet conforming to the MPEG

system standard.

[0062]

Fig. 16 shows a reception flow of integrated revocation list in preferred embodiment 2.

[0063]

In step 301,

STB receives a TS including the PES packet in which the integrated revocation list is stored.

[0064]

In step 302,

control unit 1106 sets the Revocation_pid to a PID filter of TS decoder unit 1104 so as to extract a packet including the integrated revocation list from the TS at TS decoder unit 1104 of STB.

[0065]

In step 303,

TS decoder unit 1104 extracts a packet including the integrated revocation list, and control unit 1106 obtains an integrated revocation list.

[0066]

In step 304,

control unit 1106 stores the obtained integrated revocation list in memory unit 1107.

[0067]

As a result, an integrated revocation list can be commonly shared by all STBs.

[0068]

As described herein, according to preferred embodiment 2, the apparatus is judged to be unjust if failing in the initial authentication process of the STB and the display, and the maker ID, apparatus ID, and KSV of the unjust apparatus are stored in the memory unit of the STB, and a revocation list is prepared, and from each STB, a revocation list is uploaded to the revocation list integrator via the network, and the revocation lists uploaded from the individual STBs are integrated in the revocation list integrator, and are packetized into a PES packet, and it is multiplexed into a TS, and the multiplexed TS is sent out from the transmitter, and the TS transmitted from the transmitter is received in the STB, and thereby an integrated revocation list is obtained, so that the revocation lists individually owned in each STB can be commonly possessed in all STBs, and unjust displays from the viewpoint of protection of copyright can be excluded, and the security can be enhanced.

[0069]

(Preferred embodiment 3)

Next, preferred embodiment 3 of transmission method and reception method of revocation information of the present invention is described specifically below. What differs from preferred embodiment 1 lies in the method of packetizing the integrated revocation list. Fig. 17 shows a data structure of a packet including an integrated revocation list in preferred embodiment 3. In preferred embodiment 3, as shown in Fig. 17, an integrated revocation list is stored directly in the payload of TS packet of MPEG system standard without being formed in a data structure of PES packet or section.

[0070]

Fig. 18 shows a flow of receiving an integrated revocation list in preferred embodiment 3.

[0071]

In step 401,

STB receives a TS including the packet in which the integrated revocation list is stored.

[0072]

In step 402,

control unit 1106 sets the Revocation_pid to a PID filter of TS decoder unit 1104 so as to extract a packet including the revocation list from the TS at TS decoder unit 1104 of STB.

[0073]

In step 403,

TS decoder unit 1104 extracts a packet including the integrated revocation list, and control unit 1106 obtains an integrated revocation list.

[0074]

In step 404,

control unit 1106 stores the obtained integrated revocation list in memory unit 1107.

[0075]

As a result, an integrated revocation list can be commonly shared by all STBs.

[0076]

As described herein, according to preferred embodiment 3, the

apparatus is judged to be unjust if failing in the initial authentication process of the STB and the display, and the maker ID, apparatus ID, and KSV of the unjust apparatus are stored in the memory unit of the STB, and a revocation list is prepared, and from each STB, a revocation list is uploaded to the revocation list integrator via the network, and the revocation lists uploaded from the individual STBs are integrated in the revocation list integrator, and are stored and packetized in the payload of the TS packet, and multiplexed into a TS, and the multiplexed TS is sent out from the transmitter, and the TS transmitted from the transmitter is received in the STB, and thereby an integrated revocation list is obtained, so that the revocation lists individually owned in each STB can be commonly possessed in all STBs, and unjust displays from the viewpoint of protection of copyright can be excluded, and the security can be enhanced.

[0077]

(Preferred embodiment 4)

Next, preferred embodiment 4 of transmission method and reception method of revocation information of the present invention is described specifically below. What differs from preferred embodiment 1 lies in that the integrated revocation list is transmitted to each STB via the Internet instead of digital broadcast. Fig. 19 shows a system configuration for realizing the transmission method and reception method of revocation information in preferred embodiment 4. Only the differences from preferred embodiment 1 are described below.

[0078]

Reference numerals 201 to 203 are STBs having an interface to the

Internet. Fig. 20 shows an internal configuration of STBs 201 to 203. Only the differences from the STB in preferred embodiment 1 shown in Fig. 3 are described. Reference numeral 2001 is a LAN I/F, being connected to a network described later, which is an interface for handling the IP packet.

[0079]

Reference numerals 204 to 207 are networks based on the Internet. Reference numeral 208 is a transmitting center, which stores an integrated revocation list in the IP packet. Reference numeral 209 is a transmitter, which transmits the IP packet in which the integrated revocation information is stored.

[0080]

In preferred embodiment 4 having such configuration, the operation is described below. Only the differences from preferred embodiment 1 are described below.

[0081]

In preferred embodiment 4, the operation up to preparation of revocation list by STBs 201 to 203 is same as in preferred embodiment 1. Fig. 21 shows a flow ranging from uploading to transmitting of the revocation list.

[0082]

In step 501,

control unit 1106 of the STB reads the maker ID, apparatus ID, and Bksv out of the revocation list stored in memory unit 1107, and transfers to LAN I/F 2001.

[0083]

In step 502,

Bksv is uploaded from LAN I/F 2001 of the STB to revocation list integrator 114 via networks 204, 207.

[0084]

In step 503,

revocation list integrator 114 prepares a table of Bksv uploaded from each STB during a predetermined period, and it is obtained as an integrated revocation list.

[0085]

In step 504,

the integrated revocation list is transmitted from revocation list integrator 114 to transmitting center 208.

[0086]

In step 505,

transmitting center 208 stores the integrated revocation list into an IP packet.

[0087]

In step 506,

transmitter 209 transmits the IP packet storing the integrated revocation list to each STB.

[0088]

The following is an explanation about packetizing of the integrated revocation list in step 505. Fig. 22 schematically shows an example of data structure of IP packet. In the data portion of this packet is stored integrated revocation information similar to that in preferred embodiment 1.

[0089]

Next, a method of receiving an integrated revocation list at each STB is described. Fig. 23 shows a flow of receiving an integrated revocation list at the STB.

[0090]

In step 601,

STB receives an IP packet including the integrated revocation list by means of LAN I/F 2001.

[0091]

In step 602,

control unit 1106 of the STB extracts and obtains the integrated revocation list from LAN I/F 2001.

[0092]

In step 603,

control unit 1106 stores the obtained integrated revocation list into memory unit 1107.

[0093]

As a result, an integrated revocation list can be commonly shared by all STBs.

[0094]

When a new display is connected to an STB, the operation is as follows: if the maker ID, apparatus ID, and Bksv being read out from the display coincide with those in the revocation list stored in the memory unit of the STB, the initial authentication is a failure, and the display is not usable thereafter.

[0095]

As described herein, according to preferred embodiment 4, the apparatus is judged to be unjust if failing in the initial authentication process the STB and the display, and the maker ID, apparatus ID, and KSV of the unjust apparatus are stored in the memory unit of the STB, and a revocation list is prepared, and from each STB, a revocation list is uploaded to the revocation list integrator via the network, and the revocation lists uploaded from the individual STBs are integrated in the revocation list integrator, and are packetized into an IP packet, and transmitted from the transmitter, and the IP packet transmitted from the transmitter is received in the STB, and an integrated revocation list is obtained, so that the revocation lists individually owned in each STB can be commonly possessed in all STBs, and unjust displays from the viewpoint of protection of copyright can be excluded, and the security can be enhanced.

[0096]

(Preferred embodiment 5)

Next, preferred embodiment 5 of transmission method and reception method of revocation information of the present invention is described specifically below. Fig. 24 shows a configuration of a system for realizing the transmission method and reception method of revocation information of preferred embodiment 5. What differs from preferred embodiment 1 lies in that the revocation list is not uploaded from the STB, but that the integrated revocation list is issued by revocation list integrator 301. In case of failure in the initial authentication process of a revocation list, the user reports to the revocation list controlling authority, and the revocation list controlling

authority recollects the apparatuses in which the revocation list is stored, and prepares an integrated revocation list. The integrated revocation list may be multiplexed into a TS as in preferred embodiments 1 to 3, or may be stored in the IP packet as in preferred embodiment 4. The process after preparing the integrated revocation list is same as in preferred embodiments 1 to 4.

[0097]

As described herein, according to the present preferred embodiment 5, the revocation list is not uploaded from the STB, but an integrated revocation list is prepared in the revocation list integrator, and the integrated revocation list is stored in the TS or IP packet, and is transmitted from the transmitter, and the TS transmitted from the transmitter is received in the STB, and an integrated revocation list is obtained, so that the revocation lists individually owned in each STB can be commonly possessed in all STBs, and unjust displays from the viewpoint of protection of copyright can be excluded, and the security can be enhanced.

[0098]

In the foregoing preferred embodiments, the STB is explained as a contents transmitting apparatus, but it may be DVD, PC or other apparatus. Also, as a digital interface, an example of HDMI is explained, but it may be DVI, IEEE1394, or others. The display may be also AV switcher or other repeater device. Preferably, the integrated revocation list may be stored in others than TS packet or IP packet, and transmitted. The means for uploading the revocation list is not limited to the telephone or the Internet, but may be other networks.

[0099]

[Effects of the Invention]

As described herein, according to the present invention, from the viewpoint of protection of copyright, a revocation list of unjust displays can be commonly shared by all STBs including video output apparatuses, and unjust displays can be excluded, thereby enhancing the security of the digital interface for connecting between video output apparatuses and displays.

[Brief Description of the Drawings]

Fig. 1 is a diagram showing a system for realizing a transmission method and reception method of revocation list in preferred embodiments 1 to 3.

Fig. 2 is a diagram showing an internal configuration of display.

Fig. 3 is a diagram showing an internal configuration of STB in preferred embodiments 1 to 3.

Fig. 4 is a diagram showing a matrix of device keys.

Fig. 5 is a diagram showing the process of initial authentication.

Fig. 6 is a diagram showing a revocation list possessed by STB.

Fig. 7 is a diagram showing a flow of preparation of a revocation list possessed by STB.

Fig. 8 is a diagram showing a renewed revocation list.

Fig. 9 is a diagram showing a flow ranging from uploading of revocation list to transmitting of integrated revocation list.

Fig. 10 is a diagram schematically showing a data structure of transport packet.

Fig. 11 is a diagram showing a data structure of transport packet.

Fig. 12 is a diagram showing a data structure in which an integrated revocation list is stored in a section structure.

Fig. 13 is a diagram showing a reception flow of integrated revocation list in preferred embodiment 1.

Fig. 14 is a diagram showing an integrated revocation list to be shared by each STB.

Fig. 15 is a diagram showing a data structure in which an integrated revocation list is stored in a PES packet structure.

Fig. 16 is a diagram showing a reception flow of integrated revocation list in preferred embodiment 2.

Fig. 17 is a diagram showing a data structure in which an integrated revocation list is stored in a payload of a transport packet.

Fig. 18 is a diagram showing a reception flow of integrated revocation list in preferred embodiment 3.

Fig. 19 is a diagram showing a system for realizing a transmission method and reception method of revocation list in preferred embodiment 4.

Fig. 20 is a diagram showing an internal configuration of STB in preferred embodiment 4.

Fig. 21 is a diagram showing a flow ranging from uploading of revocation list to transmitting of integrated revocation list in preferred embodiment 4.

Fig. 22 is a diagram showing a data structure of IP packet.

Fig. 23 is a diagram showing a reception flow of integrated revocation list in preferred embodiment 4.

Fig. 24 is a diagram showing a system for realizing a transmission

method and reception method of revocation list in preferred embodiment 5.

Fig. 25 is a diagram showing a background art.

[Description of the Reference Numerals and Signs]

101 first display

102 first STB

103 first digital interface

104 second display

105 second STB

106 second digital interface

107 N-th display

108 N-th STB

109 N-th digital interface

110 first up-line

111 second up-line

112 N-th up-line

113 network

114 revocation list integrator

115 transmitting center

116 transmitter

1001 display unit

1002 apparatus interface

1003 control unit

1004 memory unit

1101 antenna

1102 tuner unit

1103 front end unit

1104 TS decoder unit

1105 AV decoder unit

1106 control unit

1107 memory unit

1108 display interface

201 first STB

202 second STB

203 N-th STB

204 to 207 network

208 transmitting center

209 transmitter

2001 LAN I/F

301 revocation list integrator

[Name of the Document] Abstract

[Abstract]

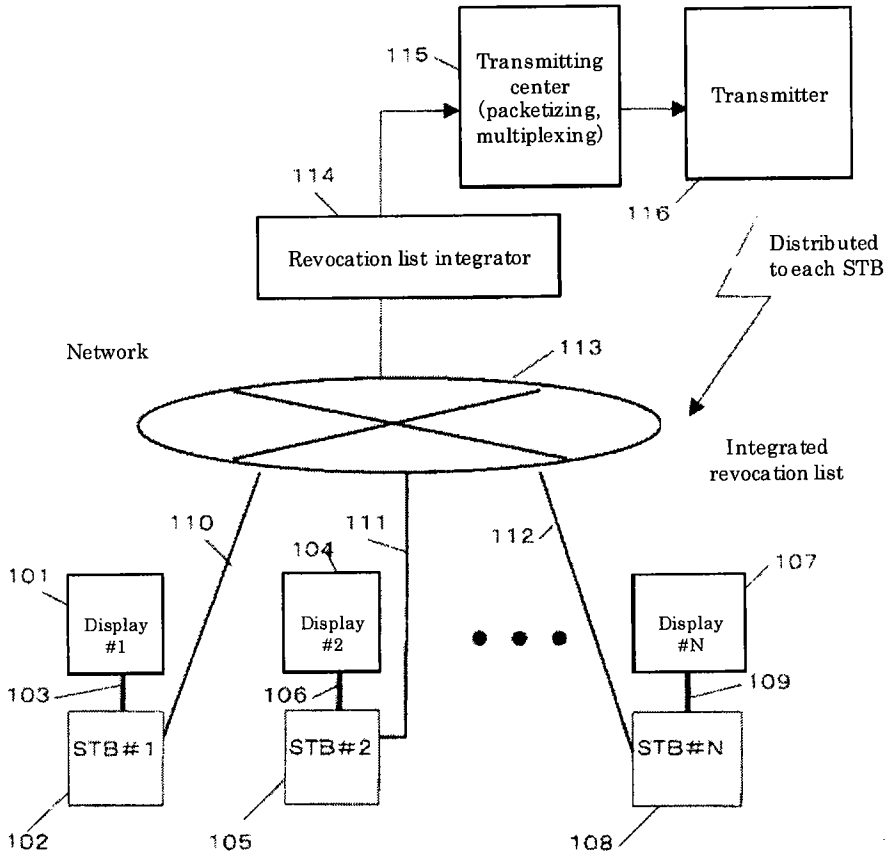
[Object] Revocation information of unjust apparatus to be excluded from the viewpoint of protection of copyright is stored only in an apparatus to be connected thereto. Instead, revocation information should be distributed to all apparatuses that may be connected, and the revocation information should be commonly shared, and unjust apparatuses must be excluded.

[Means to Solve the Problems] In a system including a contents transmitting device/ receiving device, and connecting means for connecting between them, the method includes a step of executing mutual authentication between the contents transmitting device and the contents receiving device, a step of uploading to a network, in case of failure of mutual authentication, revocation information including key information of failure, a step of preparing integrated revocation information by integrating individual revocation information uploaded from a plurality of contents transmitting devices or contents receiving devices, a step of packetizing the integrated revocation information and multiplexing it into a stream, and a step of transmitting the multiplexed stream of integrated revocation information.

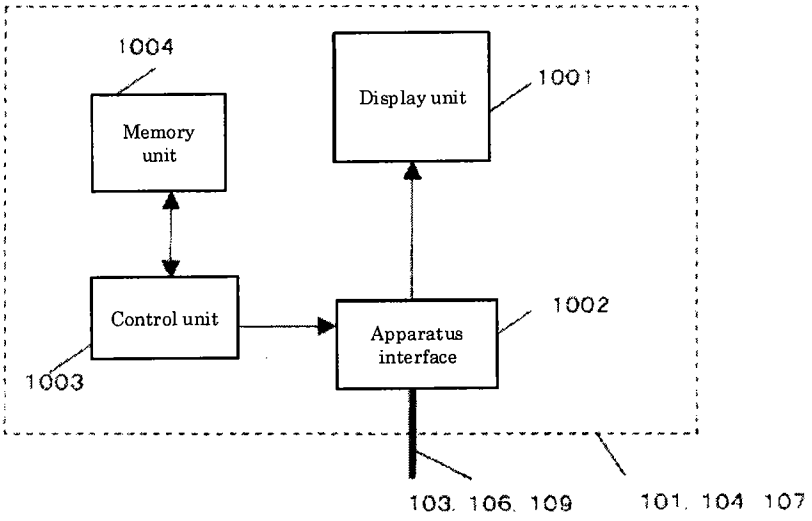
[Selected Drawing] Fig. 1.

[Name of the Document] Drawings

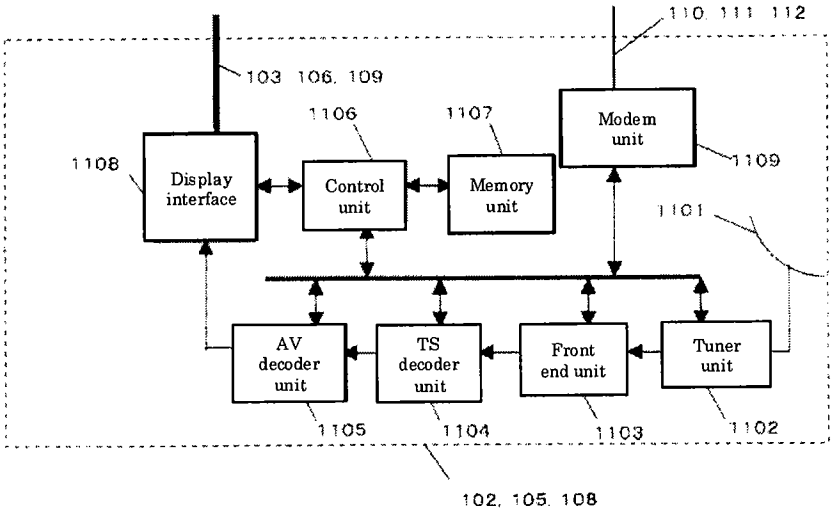
[Fig. 1]



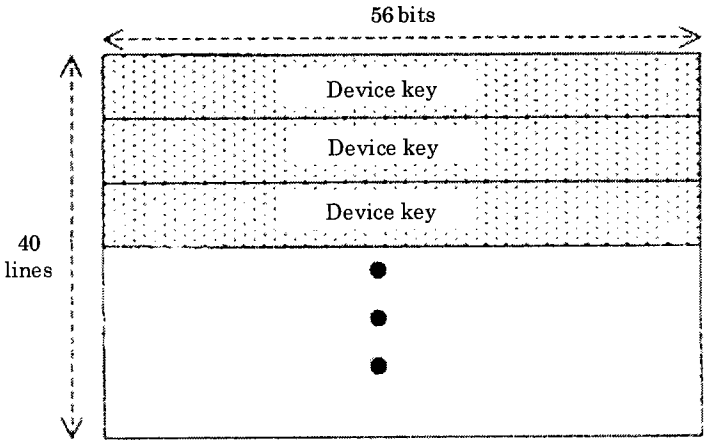
[Fig. 2]


1004
Memory unit
Display unit
1001
Control unit
1003
Apparatus interface
1002
103. 106. 109
101. 104 107

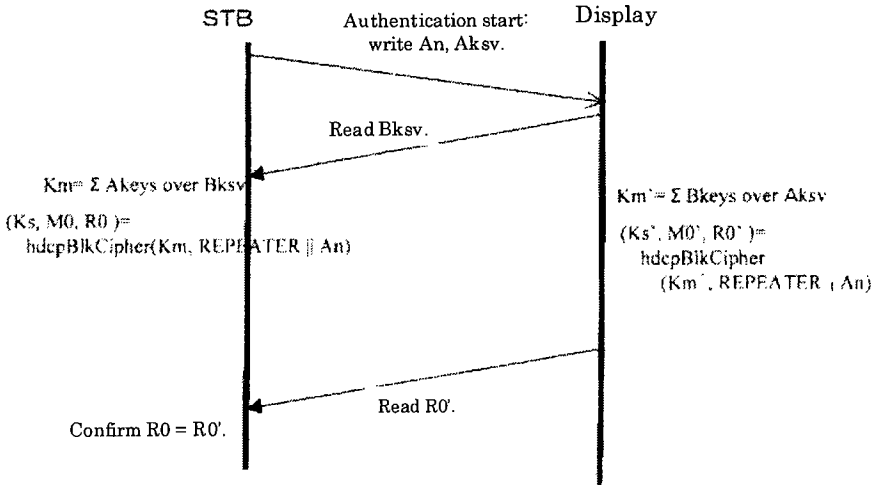
[Fig. 3]


110 111 112
103 106. 109
1106
1107
Modem unit
1108
Display interface
Control unit
Memory unit
1109
1101
AV decoder unit
TS decoder unit
Front end unit
Tuner unit
1105
1104
1103
1102
102. 105. 108

[Fig. 4]


56 bits
Device key
Device key
Device key
40
lines

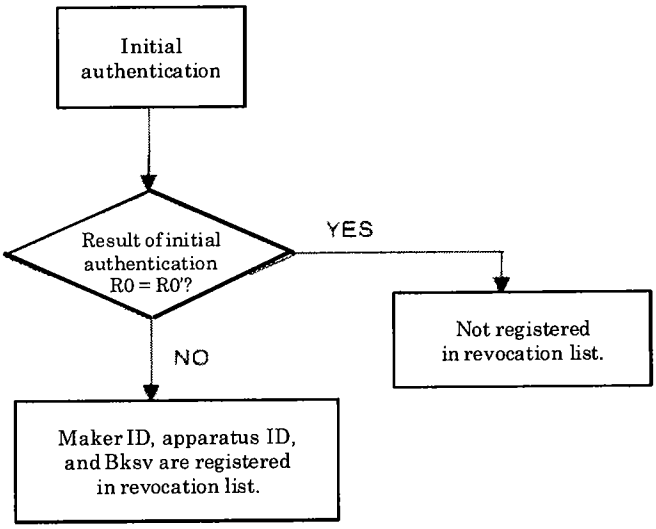
[Fig. 5]


STB
Authentication start:
write An, Aksv.
Display
Read Bksv.
Km= Σ Akeys over Bksv
(Ks, M0, R0)=
hdcpBlkCipher(Km, REPEATER || An)
Km`= Σ Bkeys over Aksv
(Ks`, M0`, R0`)=
hdcpBlkCipher
(Km`, REPEATER , An)
Read R0'.
Confirm R0 = R0'.

[Fig. 6]

Maker ID	Apparatus ID	Bksv
maker_1	kiki_1	Bksv_1
maker_2	kiki_2	Bksv_2
Not registered.	Not registered.	Not registered.
Not registered.	Not registered.	Not registered.

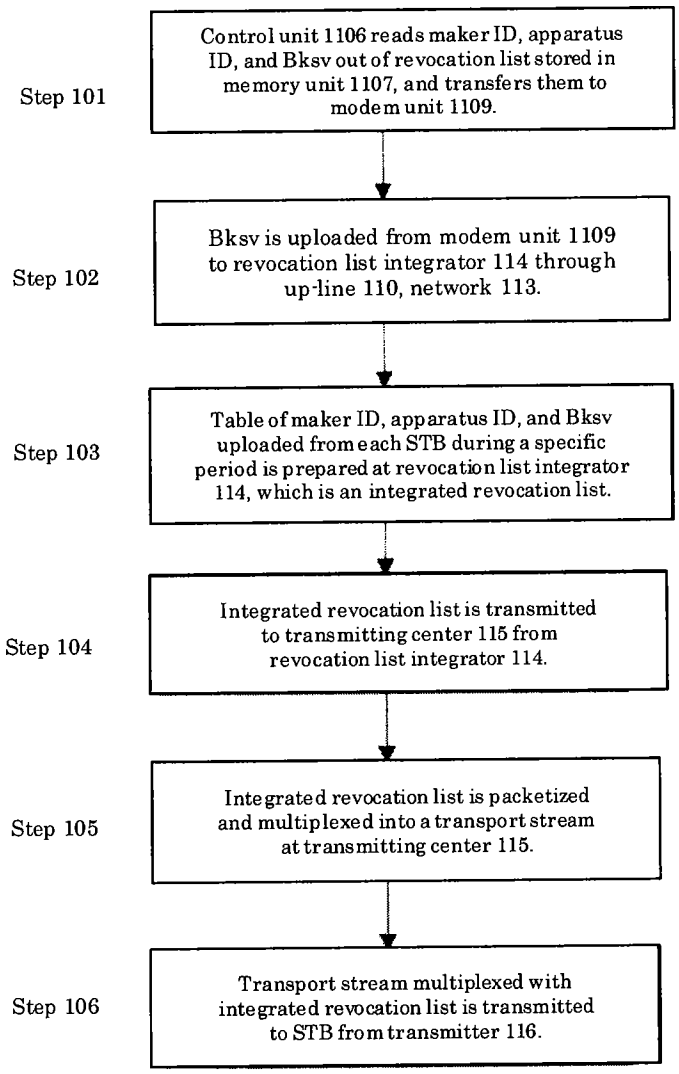
[Fig. 7]



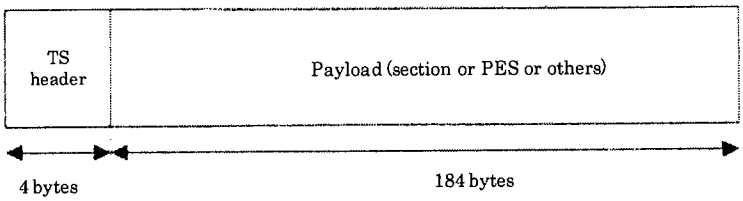
[Fig. 8]

Maker ID	Apparatus ID	Bksv
maker_1	kiki_1	Bksv_1
maker_2	kiki_2	Bksv_2
maker_3	kiki_3	Bksv_3
Not registered.	Not registered.	Not registered.

[Fig. 9]


Step 101
Control unit 1106 reads maker ID, apparatus ID, and Bksv out of revocation list stored in memory unit 1107, and transfers them to modem unit 1109.
Step 102
Bksv is uploaded from modem unit 1109 to revocation list integrator 114 through up-line 110, network 113.
Step 103
Table of maker ID, apparatus ID, and Bksv uploaded from each STB during a specific period is prepared at revocation list integrator 114, which is an integrated revocation list.
Step 104
Integrated revocation list is transmitted to transmitting center 115 from revocation list integrator 114.
Step 105
Integrated revocation list is packetized and multiplexed into a transport stream at transmitting center 115.
Step 106
Transport stream multiplexed with integrated revocation list is transmitted to STB from transmitter 116.

[Fig. 10]



[Fig. 11]

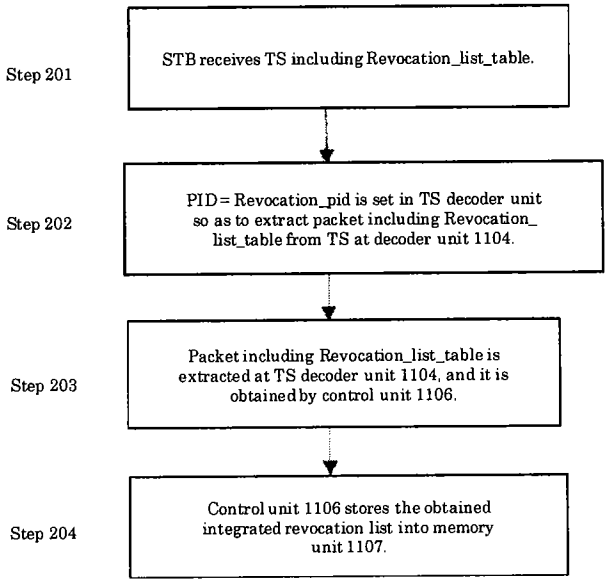
Field	No. of bits
sync_byte	8
transport_stream_indicatior	1
payload_unit_start_indicator	1
tranport_priority	1
PID	13
transport_scrambling_cintrol	2
adaptation_field_control	2
continuity_counter	4
for (i=0; i <n; i++){	
data_byte	8
}	

[Fig. 12]

Revocation_List_Table

Field	No. of bits
table_id	8
section_syntax_indicatior	1
reserved	2
section_length	12
program_number	16
reserved	2
version_number	5
current_next_indicator	1
section_number	8
last_section_number	8
for(i=0; i<n; i++){	
maker id	16
kiki_id	32
device_KSV	40
}	
CRC_32	32

[Fig. 13]



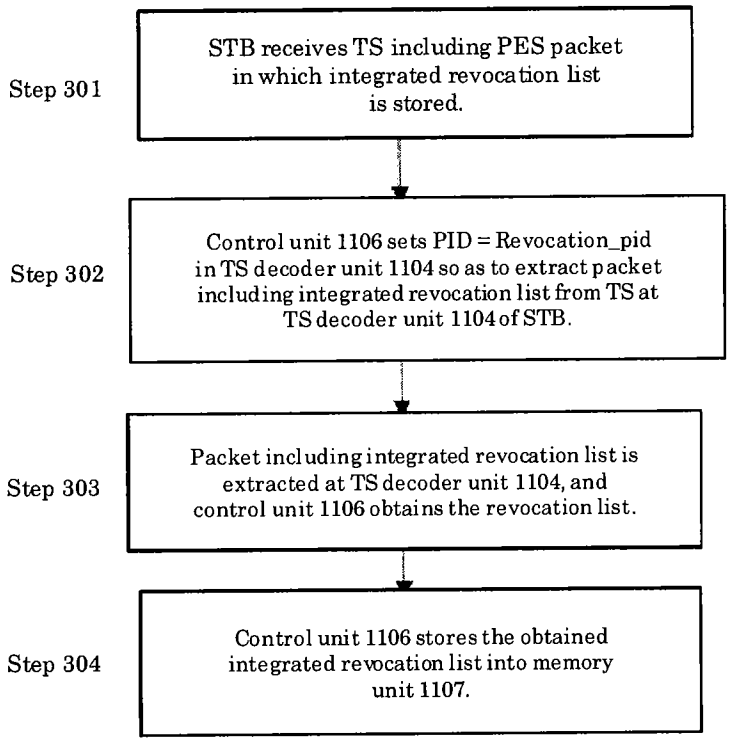
[Fig. 14]

Maker ID	Apparatus ID	Bksv
maker_1	kiki_1	Bksv_1
maker_2	kiki_2	Bksv_2
maker_3	kiki_3	Bksv_3
maker_4	kiki_4	Bksv_4
maker_5	kiki_5	Bksv_5
Not registered.	Not registered.	Not registered.
Not registered.	Not registered.	Not registered.

[Fig. 15]

Field	No. of bits
packet_start_code_prefix	24
strem_id	8
PES_packet_lengh	16
for (i=0; i<PES_packet_length/5; i++){	
maker_id	16
kiki_id	32
device_KSV	40
}	

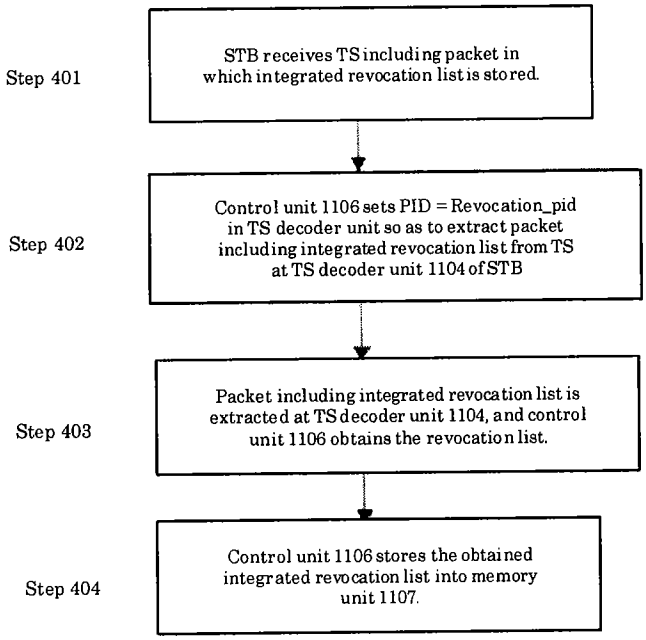
[Fig. 16]



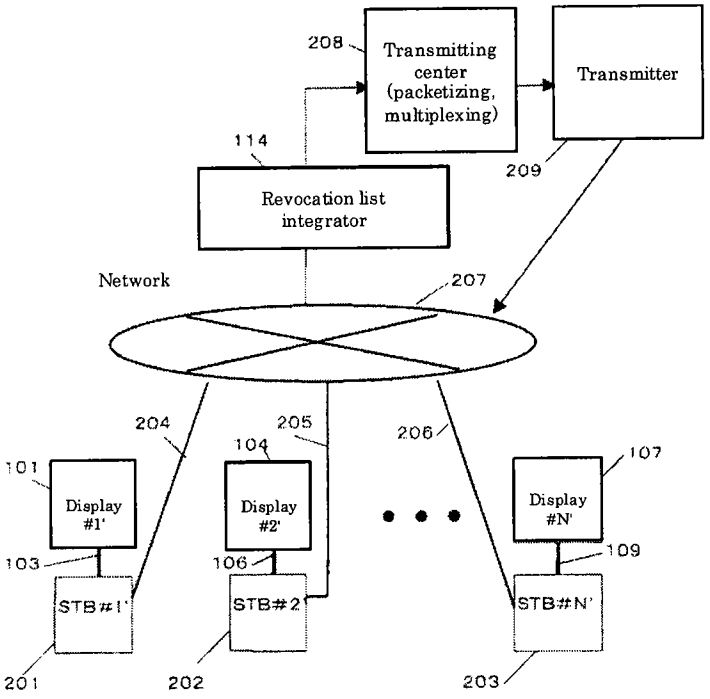
[Fig. 17]

Field	No. of bits
KSV_number	16
For (I=0; I<KSV_number; I++){	
maker_id	16
kiki_id	32
device_KSV	40
}	

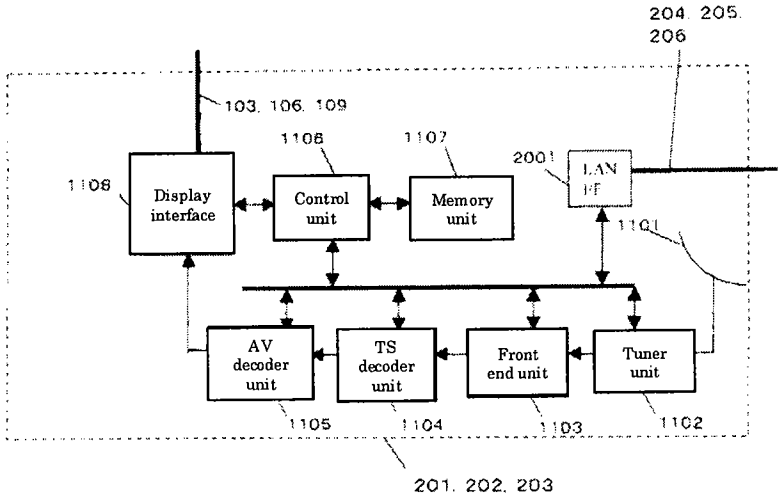
[Fig. 18]


Step 401
STB receives TS including packet in which integrated revocation list is stored.
Step 402
Control unit 1106 sets PID = Revocation_pid in TS decoder unit so as to extract packet including integrated revocation list from TS at TS decoder unit 1104 of STB
Step 403
Packet including integrated revocation list is extracted at TS decoder unit 1104, and control unit 1106 obtains the revocation list.
Step 404
Control unit 1106 stores the obtained integrated revocation list into memory unit 1107.

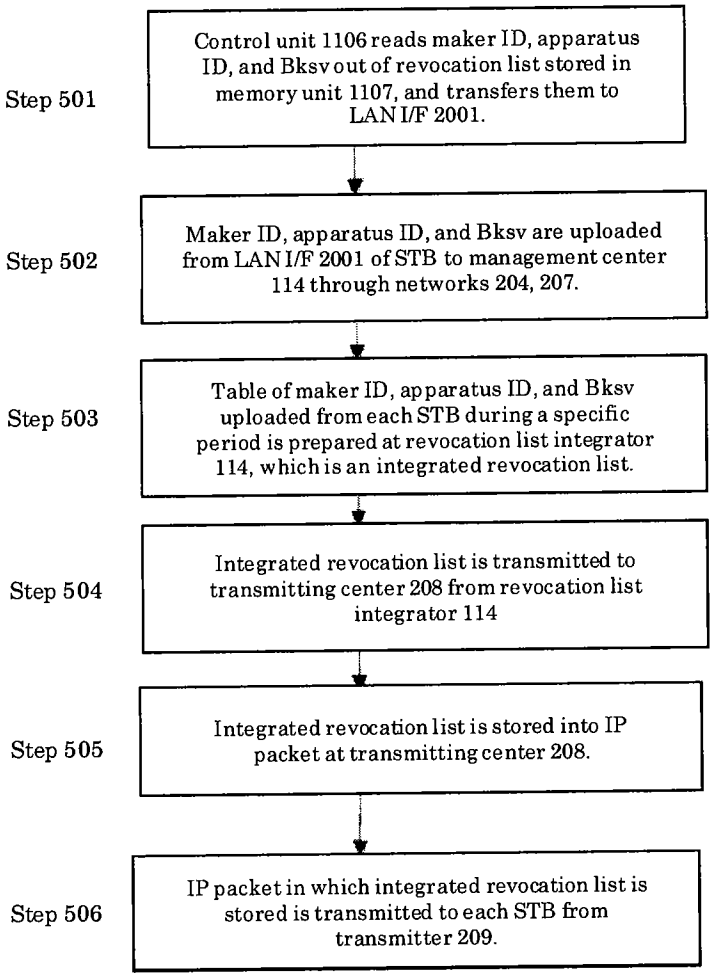
[Fig. 19]


208
Transmitting center (packetizing, multiplexing)
Transmitter
209
114
Revocation list integrator
Network
207
204
205
206
101
Display #1'
104
Display #2'
107
Display #N'
103
106
109
STB#1'
STB#2
STB#N'
201
202
203

[Fig. 20]


204. 205. 206
103. 106. 109
1108
1107
2001
1108
Display interface
Control unit
Memory unit
LAN I/F
1101
AV decoder unit
TS decoder unit
Front end unit
Tuner unit
1105
1104
1103
1102
201. 202. 203

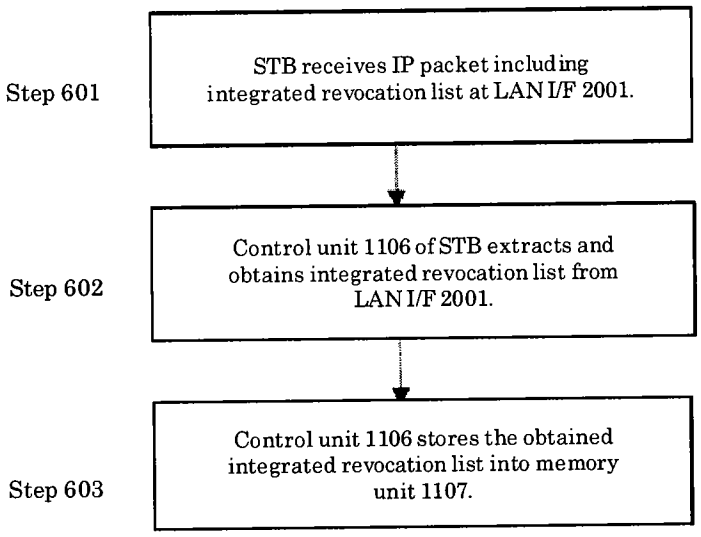
[Fig. 21]



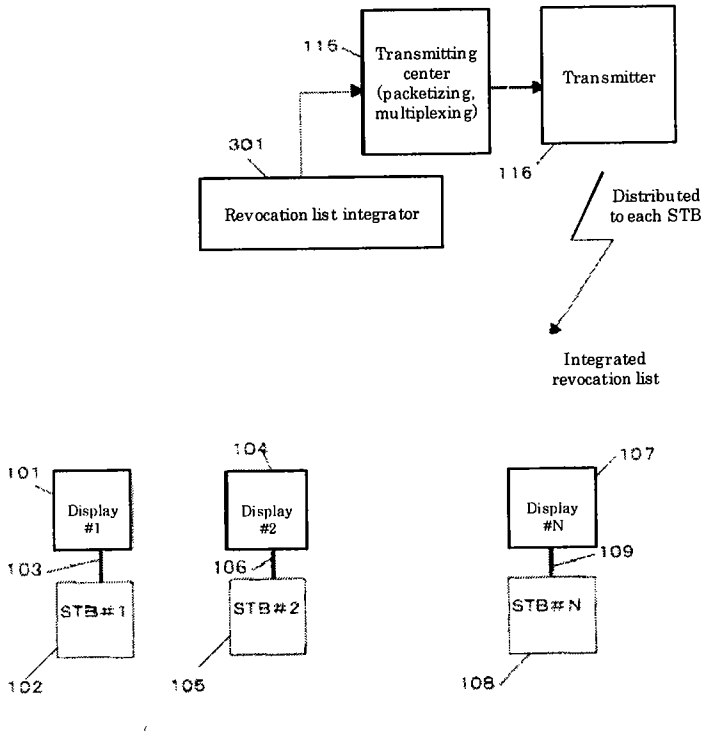
[Fig. 22]

Transmit IP address	Receive IP address	Protocol type	Transmit port No.	Receive port No.	Data	FCS

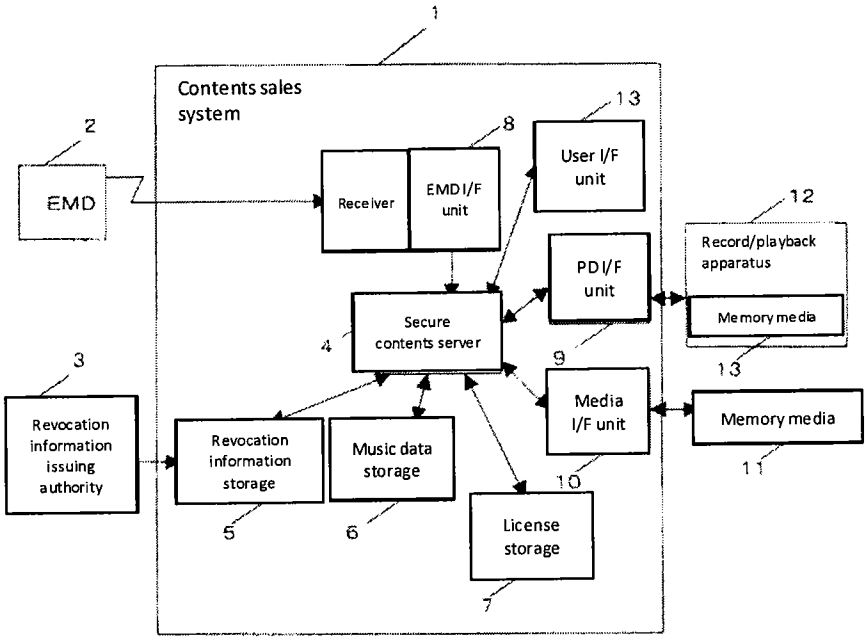
[Fig. 23]


Step 601
STB receives IP packet including integrated revocation list at LAN I/F 2001.
Step 602
Control unit 1106 of STB extracts and obtains integrated revocation list from LAN I/F 2001.
Step 603
Control unit 1106 stores the obtained integrated revocation list into memory unit 1107.

[Fig. 24]


115
Transmitting center (packetizing, multiplexing)
Transmitter
116
301
Revocation list integrator
Distributed to each STB
Integrated revocation list
101
Display #1
103
STB#1
102
104
Display #2
106
STB#2
105
107
Display #N
109
STB#N
108

[Fig. 25]


1
Contents sales system
2
EMD
8
Receiver
EMD I/F unit
13
User I/F unit
12
Record/playback apparatus
Memory media
PD I/F unit
4
Secure contents server
9
13
3
Revocation information issuing authority
Media I/F unit
Memory media
11
Revocation information storage
Music data storage
10
License storage
5
6
7